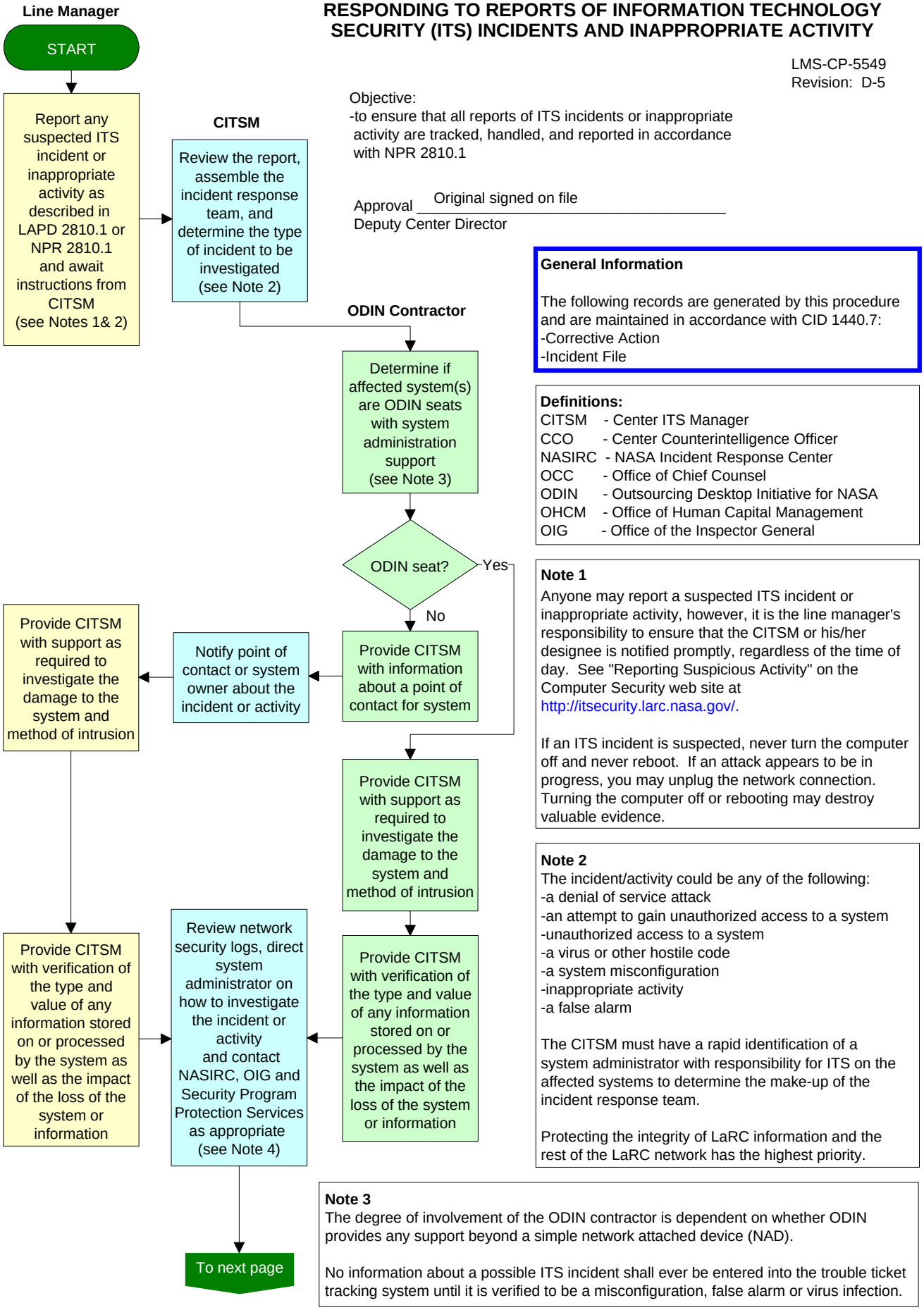
RESPONDING TO REPORTS OF INFORMATION TECHNOLOGY SECURITY (ITS) INCIDENTS AND INAPPROPRIATE ACTIVITY

LMS-CP-5549
Revision: D-5

Objective:
-to ensure that all reports of ITS incidents or inappropriate activity are tracked, handled, and reported in accordance with NPR 2810.1

Approval Original signed on file
Deputy Center Director



General Information

The following records are generated by this procedure and are maintained in accordance with CID 1440.7:
-Corrective Action
-Incident File

Definitions:

CITSM	- Center ITS Manager
CCO	- Center Counterintelligence Officer
NASIRC	- NASA Incident Response Center
OCC	- Office of Chief Counsel
ODIN	- Outsourcing Desktop Initiative for NASA
OHCM	- Office of Human Capital Management
OIG	- Office of the Inspector General

Note 1

Anyone may report a suspected ITS incident or inappropriate activity, however, it is the line manager's responsibility to ensure that the CITSM or his/her designee is notified promptly, regardless of the time of day. See "Reporting Suspicious Activity" on the Computer Security web site at http://itsecurity.larc.nasa.gov/.

If an ITS incident is suspected, never turn the computer off and never reboot. If an attack appears to be in progress, you may unplug the network connection. Turning the computer off or rebooting may destroy valuable evidence.

Note 2

The incident/activity could be any of the following:
-a denial of service attack
-an attempt to gain unauthorized access to a system
-unauthorized access to a system
-a virus or other hostile code
-a system misconfiguration
-inappropriate activity
-a false alarm

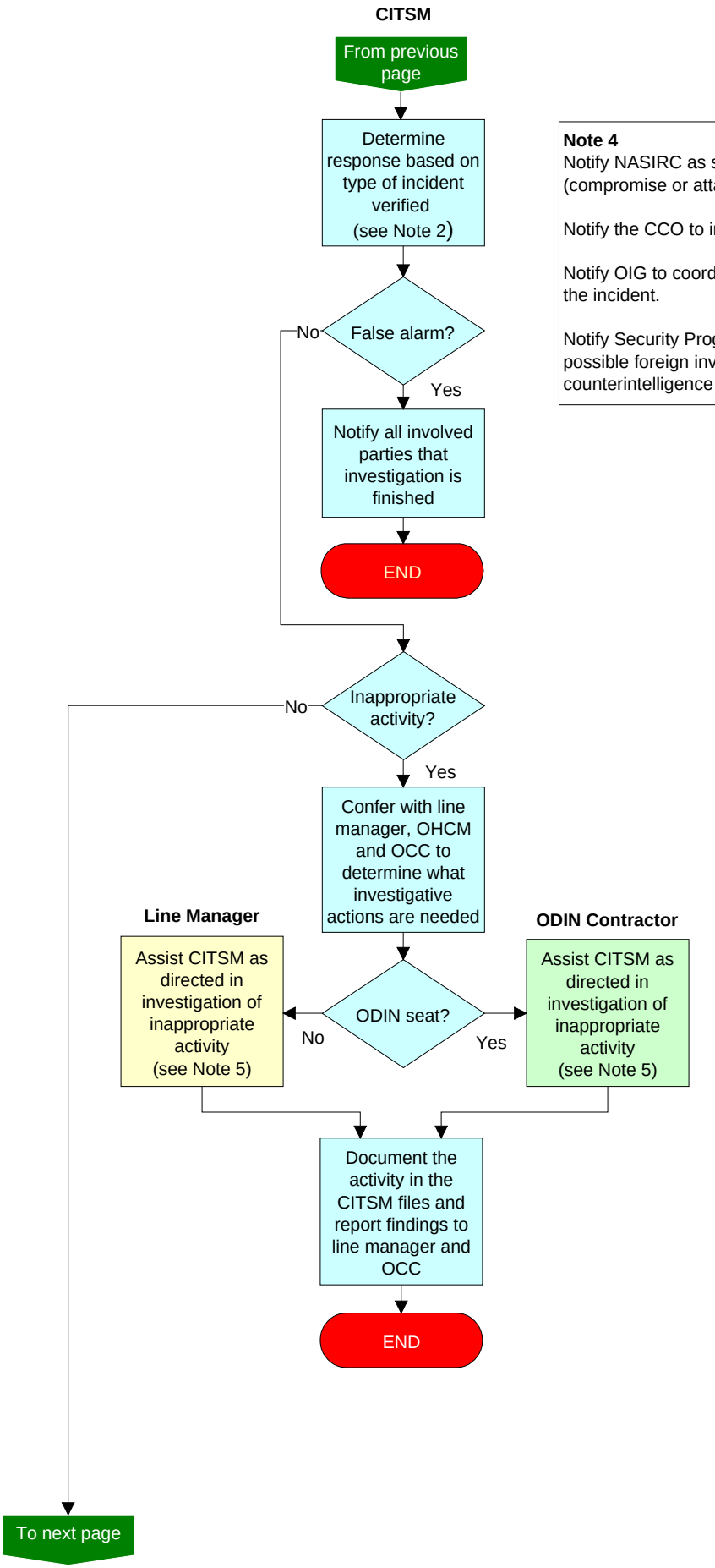
The CITSM must have a rapid identification of a system administrator with responsibility for ITS on the affected systems to determine the make-up of the incident response team.

Protecting the integrity of LaRC information and the rest of the LaRC network has the highest priority.

Note 3

The degree of involvement of the ODIN contractor is dependent on whether ODIN provides any support beyond a simple network attached device (NAD).

No information about a possible ITS incident shall ever be entered into the trouble ticket tracking system until it is verified to be a misconfiguration, false alarm or virus infection.



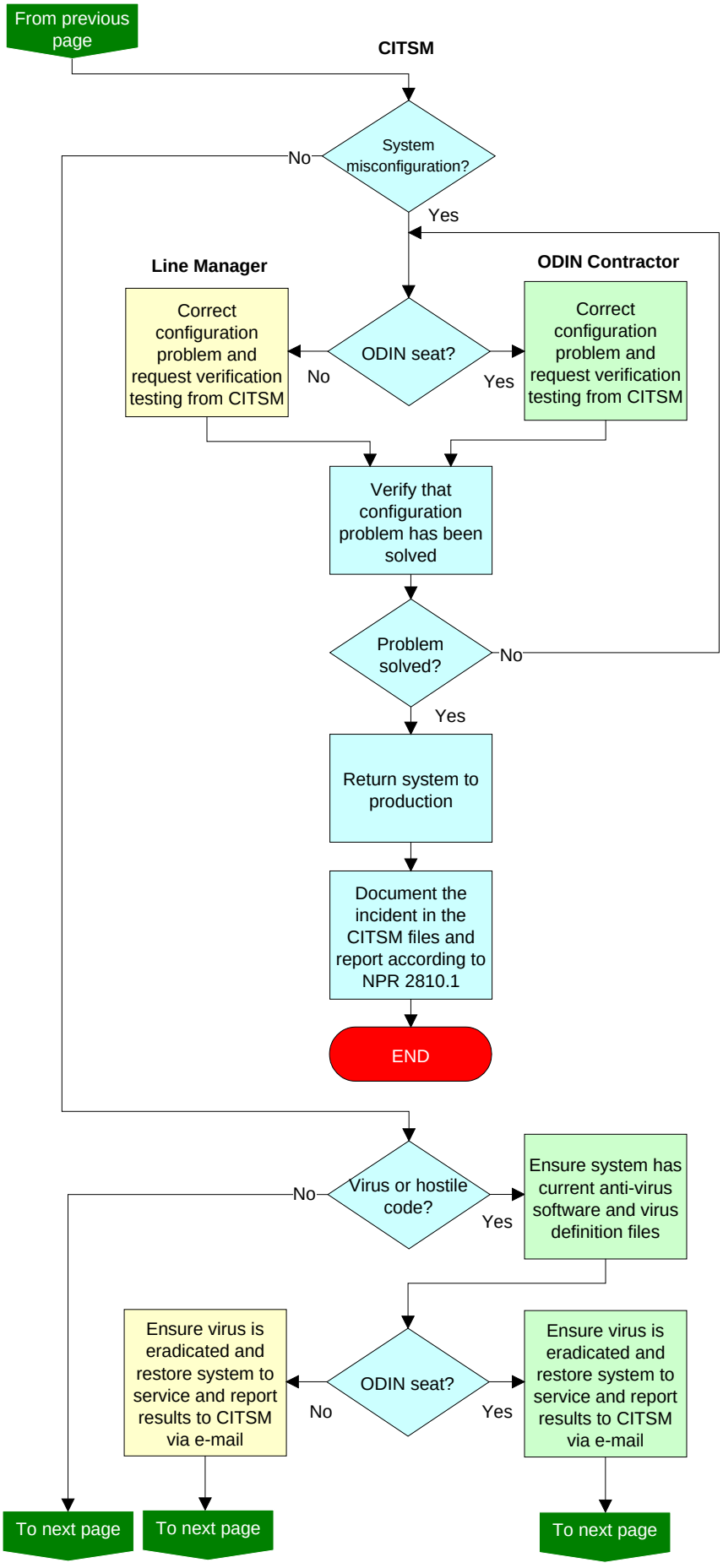
Note 4
Notify NASIRC as soon as the CITSM is reasonably certain that an ITS incident (compromise or attack) is verified.

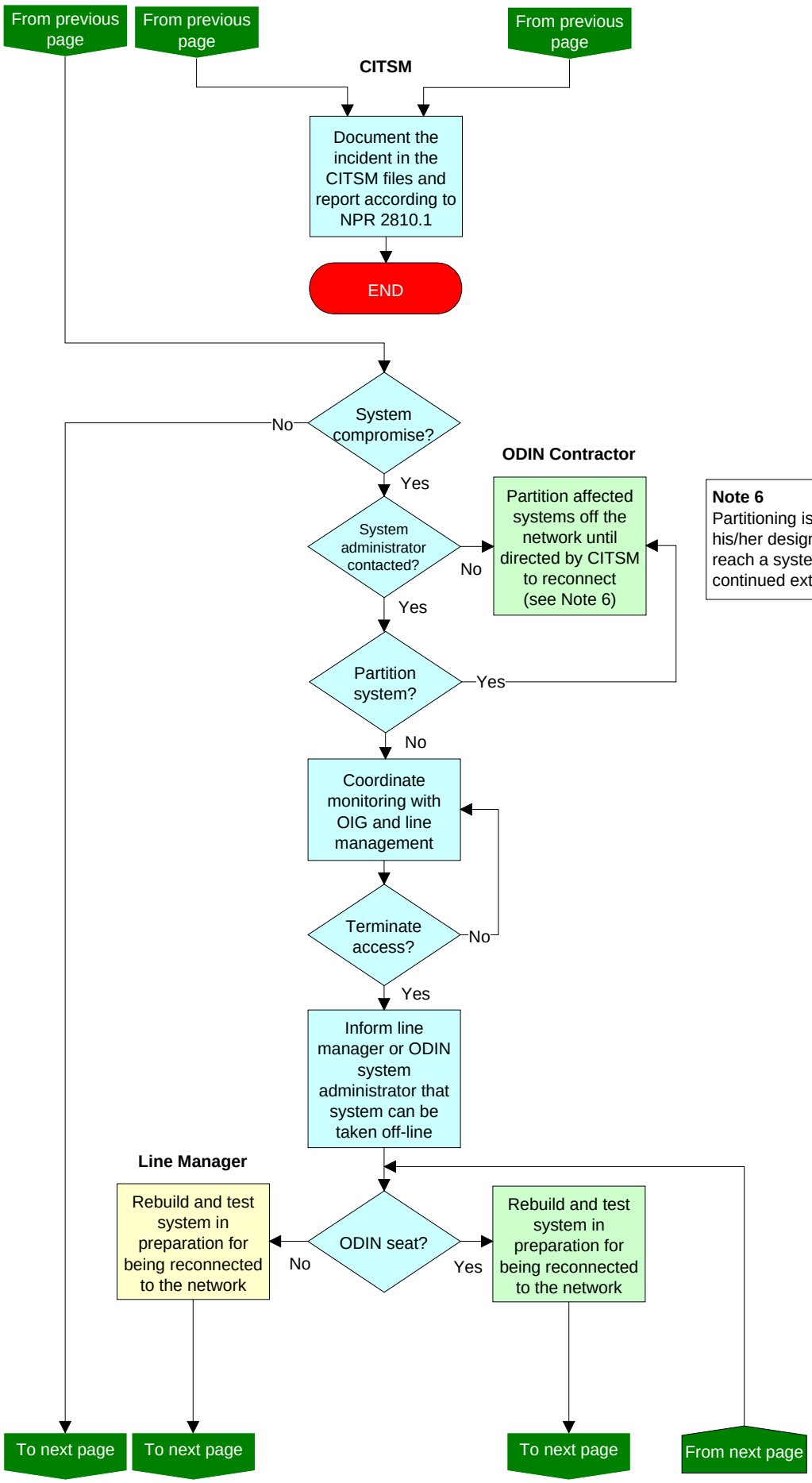
Notify the CCO to investigate for signs of foreign involvement in the incident.

Notify OIG to coordinate monitoring or if there is evidence of criminal activity in the incident.

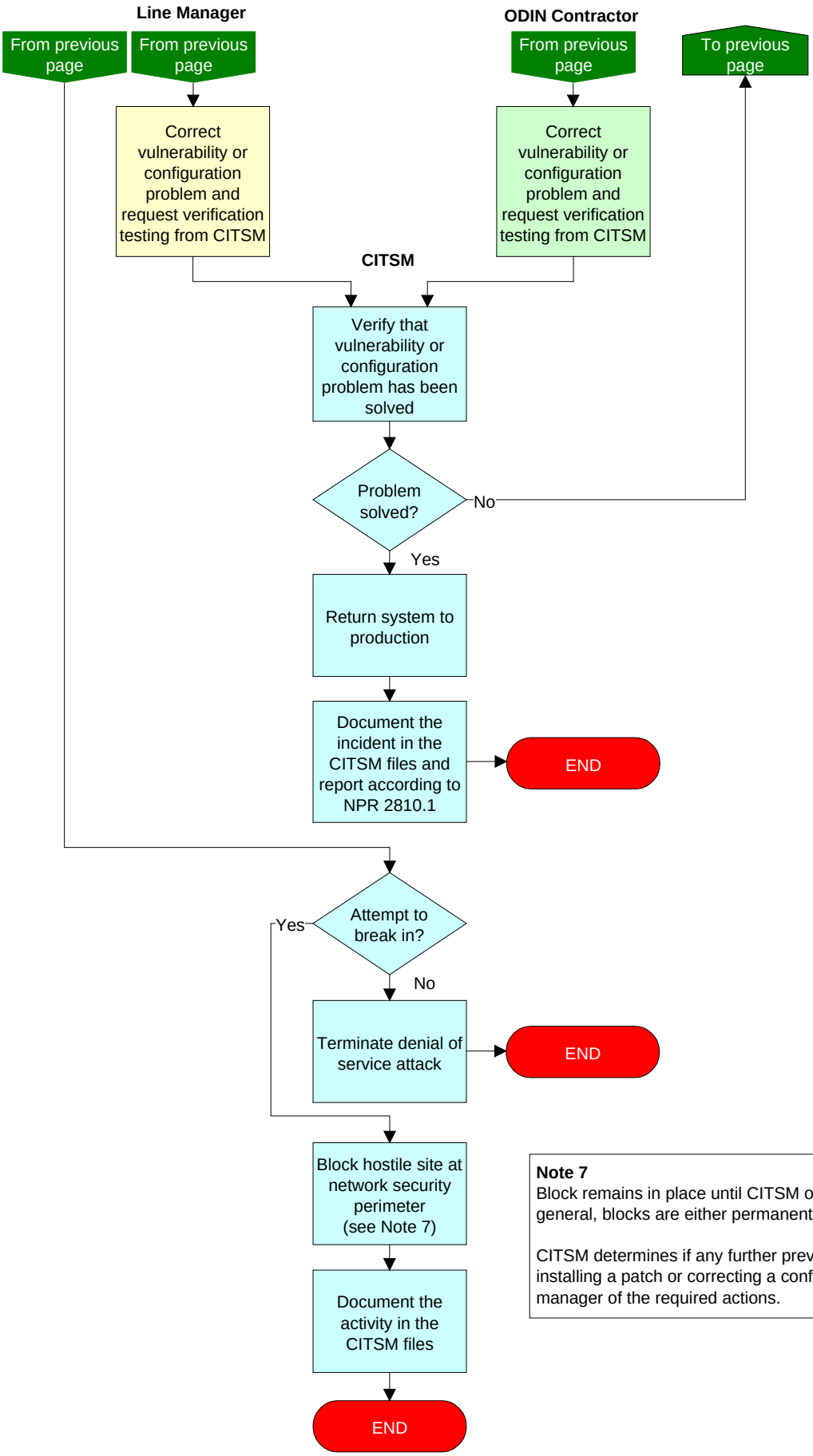
Notify Security Program Protection Services if there is any evidence to support possible foreign involvement in the incident with the possibility of counterintelligence information gathering.

Note 5
This activity is highly confidential and any information gathered must be protected.


From previous page
CITSM
System misconfiguration?
No
Yes
Line Manager
ODIN Contractor
Correct configuration problem and request verification testing from CITSM
ODIN seat?
No
Yes
Correct configuration problem and request verification testing from CITSM
Verify that configuration problem has been solved
Problem solved?
No
Yes
Return system to production
Document the incident in the CITSM files and report according to NPR 2810.1
END
Virus or hostile code?
No
Yes
Ensure system has current anti-virus software and virus definition files
Ensure virus is eradicated and restore system to service and report results to CITSM via e-mail
ODIN seat?
No
Yes
Ensure virus is eradicated and restore system to service and report results to CITSM via e-mail
To next page
To next page
To next page



Note 6
Partitioning is an emergency step directed by CITSM or his/her designee when it is impossible or impractical to reach a system administrator for the system and the continued external attack must be halted.



Note 7
Block remains in place until CITSM or his/her designee directs removal. In general, blocks are either permanent or for 30, 60, or 90 days.

CITSM determines if any further preventative actions are necessary, such as installing a patch or correcting a configuration file and notifies the line manager of the required actions.